On the Asymptotic Weight Distribution of Regular LDPC Ensembles

Vishwambhar Rathi
EPFL
Lausanne 1015, Switzerland
Email: vishwambhar.rathi@epfl.ch

***Abstract*— We estimate the variance of weight distribution of regular LDPC ensembles. Using this estimate and the second moment method we obtain bounds on the probability that a randomly chosen code from regular LDPC ensemble has its weight distribution close to the ensemble average. We are able to show that a large fraction of total number of codes have their weight distribution close to the average.**

I. Introduction

The weight distribution is an important characterization of a code. For a code G of block length n, we define $N(G,n\omega)$ as the weight distribution function, denoting the number of codewords with normalized weight ω (here on wards we assume that $n\omega$ is an integer). In general $N(G,n\omega)$ is hard to compute for a specific code. In fact, even the determination of the minimum distance is NP-complete [13]. On the contrary, for some ensembles of codes it is easy to compute the *expected* weight distribution function, i.e., $\mathbb{E}[N(G,n\omega)]$. This is true for e.g. Shannon's random ensemble but also for suitably defined LDPC ensembles. A possible approach to study the weight distribution of *individual* codes is to first compute the ensemble average and then to show that most codes have a weight distribution close to this average. For LDPC codes it has been conjectured that for regular ensembles most codes have a weight distribution close to the ensemble average [2], [10].

In 1989, Sourlas showed that there is a strong connection between error-correcting codes and disordered spin models [11], [12]. To this end, let us define:

$$W_{\mathrm{sp}}(\omega) = \lim_{n\to\infty} \frac{\mathbb{E}[\ln N(G,n\omega)]}{n},\ W_{\mathrm{com}}(\omega) = \lim_{n\to\infty} \frac{\ln \mathbb{E}[N(G,n\omega)]}{n},$$

where sp stands for "statistical physics", since $W_{\mathrm{sp}}(\omega)$ can be computed by statistical physics methods and com stands for "combinatorics", as $W_{\mathrm{com}}(\omega)$ can easily be computed by combinatorial methods. From Jensen's inequality we know that $W_{\mathrm{sp}}(\omega) \le W_{\mathrm{com}}(\omega)$. It has been shown in [2], [10] that for regular LDPC ensembles $W_{\mathrm{sp}}(\omega) = W_{\mathrm{com}}(\omega)$. However for irregular LDPC ensembles this is not the case [4]. The equality between $W_{\mathrm{com}}(\omega)$ and $W_{\mathrm{sp}}(\omega)$ for regular ensembles suggests that a randomly chosen code should have $N(G,n\omega)$ "close" to $\mathbb{E}[N(G,n\omega)]$ with high probability. In this paper we obtain an asymptotic lower bound on this probability using the second moment method by estimating the variance of $N(G,n\omega)$. However, to estimate the variance we need to verify that the solution set of a certain system of polynomial equations satisfies some properties (see Lemma 3.4 for details). Assuming that these properties are satisfied, we show that for a regular LDPC ensemble with left degree $\mathtt{l}$ and right degree $\mathtt{r}$, any $\varepsilon > 0$ and for all ω such that $W_{\mathrm{com}}(\omega)$ is positive,

$$\lim_{n\to\infty} \mathrm{P}\left(1-\varepsilon \le \frac{N(G,n\omega)}{\mathbb{E}[N(G,n\omega)]} \le 1+\varepsilon\right) \ge 1 - \frac{\delta(\omega,\mathtt{l},\mathtt{r})}{\varepsilon^2}, \quad (1)$$

where $\delta(\omega,\mathtt{l},\mathtt{r})$ is a function of ω and can be evaluated by solving a polynomial equation.

In words, asymptotically at least a fraction $1-\frac{\delta(\omega,\mathtt{l},\mathtt{r})}{\varepsilon^2}$ of codes in the ensemble have their weight distribution function in a window of width ε around the ensemble average. In Fig. 1 we plot the bound in (1) for regular codes with $\mathtt{l}/\mathtt{r} = 0.75$ and 0.5. We observe that if we fix the ratio $\mathtt{l}/\mathtt{r}$ and let $\mathtt{l},\mathtt{r}$ increase then the bound converges to 1. This implies that for large left and right degrees, almost all the codes in the ensemble have their weight distribution very close to the ensemble average. Note that in this case it is well known that the weight distribution converges to the weight distribution of Shannon's random ensemble [9].

The paper is organized in the following way. A brief introduction to LDPC codes and second moment method is given in Section 2. In Section 3, we use the second moment method to prove the bound in (1). A discussion in Section 4 concludes the paper.

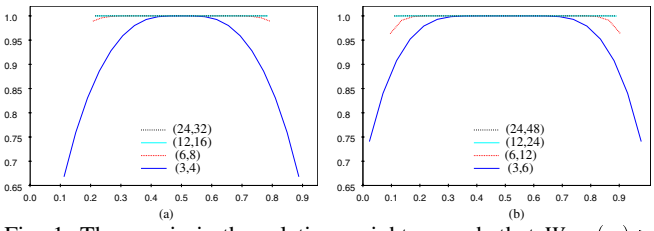

Fig. 1: The x-axis is the relative weight ω such that $W_{\mathrm{com}}(\omega) > 0$ and y-axis is the bound $1-\frac{\delta(\omega,\mathtt{l},\mathtt{r})}{\varepsilon^2}$ with $\varepsilon = 0.95$, (a) for ensembles with rate=0.25, (b) for ensembles with rate=0.5.

II. Preliminaries

A. LDPC Ensembles

LDPC codes, originally invented by Gallager [7], are usually defined in terms of ensembles of *bipartite graphs*. A graph consists of a set of *variable* nodes and a set of *check* nodes, together with edges connecting both sets giving rise to a code of block length n in the following way: a vector $(x_1,\cdots,x_n) \in \mathrm{GF}(2)^n$ is a codeword if and only if for each check node the sum (modulo 2) of the values of its adjacent variable nodes is zero. The coordinates of a codeword are indexed by the variable nodes $1,\cdots,n$. An ensemble of bipartite graphs is defined in terms of a pair of *degree distributions*. A degree distribution is a real valued polynomial with non-negative

coefficients and it evaluates to unity at unity. Associated with the ensemble is a degree distribution pair $(\lambda(x) = \Sigma_i \lambda_i x^{i-1}, \rho(x) = \Sigma_j \rho_j x^{j-1})$, shorthand (λ, ρ), where λ_i (ρ_j) denotes the fraction of the total number of edges connected to a variable (check) node of degree i (j). Given a pair (λ, ρ) of degree distributions and the block length n, an *ensemble* of bipartite graphs $\mathbb{G}(n, \lambda, \rho)$ is defined by running over all possible permutations of edges connecting variable and check nodes according to λ and ρ, respectively. For a $(\mathtt{l}, \mathtt{r})$-regular code ensemble $\mathbb{G}(n, \mathtt{l}, \mathtt{r})$ we have: $\lambda(x) = x^{\mathtt{l}-1}, \rho(x) = x^{\mathtt{r}-1}$. Let G be a graph chosen at random from $\mathbb{G}(n, \mathtt{l}, \mathtt{r})$. Let $N(G, n\omega)$ be the weight distribution function denoting the number of codewords of weight $n\omega$ in G where $\omega = W/n$ is the normalized weight with W denoting the weight. Let $\sigma^2(G, n\omega)$ denote the variance of $N(G, n\omega)$ over the ensemble $\mathbb{G}(n, \mathtt{l}, \mathtt{r})$, $\sigma^2(G, n\omega) = \mathbb{E}[N(G, n\omega)^2] - \mathbb{E}[N(G, n\omega)]^2$. The *support set* of a word is the set of its non zero bits. The *overlap* between two words is the intersection of their support sets. We denote a vector (x_1, x_2, x_3) by $\underline{x}$, the transpose of $\underline{x}$ by $\underline{x}^T$, the dot product between $\underline{x}$ and $\underline{y}$ is denoted by $\underline{x}.\underline{y}^T$, $\underline{xy}$ denotes the component wise multiplication, i.e., the vector (x_1y_1, x_2y_2, x_2y_3). We use the notation that a vector to the power a vector and also a scalar to the power a vector is a vector i.e. , $\underline{x}^{\underline{k}} := (x_1^{k_1}, x_2^{k_2}, x_3^{k_3})$ and $e^{\underline{x}} := (e^{x_1}, e^{x_2}, e^{x_3})$. Finally, $x^+ := \max(x, 0)$ and $f'(t)$ denotes the derivative of the function $f(x)$ evaluated at t.

B. Second Moment Method

Let $\{X_n\}$ be a sequence of random variables indexed by n, $n \in \mathbb{N}$. Let $\sigma_n^2 = \mathbb{E}[(X_n - \mathbb{E}[X_n])^2]$ be the variance of X_n. Then by Chebyshev's inequality we have for any $a \geq 0$,

$$\mathrm{P}(|X_n - \mathbb{E}[X_n]| \geq a) \leq \frac{\sigma_n^2}{a^2}.$$

If we choose $a = \varepsilon \mathbb{E}[X_n]$ and if $\lim_{n\to\infty} \frac{\sigma_n^2}{\mathbb{E}[X_n]^2} = \delta$, then we can draw the conclusion that

$$\lim_{n\to\infty} \mathrm{P}\left(1 - \varepsilon \leq \frac{X_n}{\mathbb{E}[X_n]} \leq 1 + \varepsilon\right) \geq 1 - \frac{\delta}{\varepsilon^2}.$$

In order to apply this bound to $N(G, n\omega)$, we need to compute the ratio $\lim_{n\to\infty} \frac{\sigma^2(G,n\omega)}{\mathbb{E}[N(G,n\omega)]^2} = \lim_{n\to\infty} \frac{\mathbb{E}[N^2(G,n\omega)]}{\mathbb{E}[N(G,n\omega)]^2} - 1$.

III. Moment Calculations

We start with the first moment. As shown in [3], [5], [8],

$$\mathbb{E}[N(G, n\omega)] = \frac{\binom{n}{n\omega}}{\binom{n\mathtt{l}}{n\mathtt{l}\omega}} \mathrm{Coeff}\left(p(x)^{\frac{\mathtt{l}n}{\mathtt{r}}}, x^{n\mathtt{l}\omega}\right), \tag{2}$$

where $\mathrm{Coeff}(p(x)^{\frac{n\mathtt{l}}{\mathtt{r}}}, x^{n\mathtt{l}\omega})$ denotes the coefficient of $x^{n\mathtt{l}\omega}$ in the Taylor series expansion of $p(x)^{\frac{n\mathtt{l}}{\mathtt{r}}}$ and $p(x) = ((1+x)^{\mathtt{r}} + (1-x)^{\mathtt{r}})/2$. We note that $p(x)$ has only even powers of x. To remove this periodicity of powers, we define the polynomial $q(x) = p(\sqrt{x})$. Now, $\mathrm{Coeff}(p(x)^{\frac{n\mathtt{l}}{\mathtt{r}}}, x^{n\mathtt{l}\omega}) = \mathrm{Coeff}(q(x)^{\frac{n\mathtt{l}}{\mathtt{r}}}, x^{\frac{n\mathtt{l}\omega}{2}})$. In the next lemma, we recall the Hayman method to approximate $\mathrm{Coeff}(q(x)^{\frac{n\mathtt{l}}{\mathtt{r}}}, x^{\frac{n\mathtt{l}\omega}{2}})$ for large values of n, a proof of which can be found in [6].

Lemma 3.1: [Hayman Method] Let $q(x) = \sum_i q_i x^i$ be a polynomial with non negative coefficients such that $q_0 \neq 0$ and $q_1 \neq 0$. Define $a_q(x) := x\frac{q'(x)}{q(x)}$ and $b_q(x) := x a_q'(x)$. Then for n tending to infinity so that $\frac{n\mathtt{l}\omega}{2} \in \mathbb{N}$

$$\mathrm{Coeff}(q(x)^{\frac{n\mathtt{l}}{\mathtt{r}}}, x^{\frac{n\mathtt{l}\omega}{2}}) = \frac{q(t_\omega)^{\frac{n\mathtt{l}}{\mathtt{r}}}}{(t_\omega)^{\frac{n\mathtt{l}\omega}{2}} \sqrt{2\pi \frac{n\mathtt{l}}{\mathtt{r}} b_q(t_\omega)}} (1 + o(1)), \tag{3}$$

where the term $o(1)$ converges to zero and t_ω is the unique positive solution of $a_q(x) = \frac{\mathtt{r}\omega}{2}$.

Since $q(x) = p(\sqrt{x})$, we have $a_q(x) = a_p(\sqrt{x})/2$, $b_q(x) = b_p(\sqrt{x})/4$. Also $t_\omega = x_\omega^2$, where x_ω is the unique positive solution of $a_p(x) = r\omega$ which simplifies to,

$$x\frac{(1+x)^{\mathtt{r}-1} - (1-x)^{\mathtt{r}-1}}{(1+x)^{\mathtt{r}} + (1-x)^{\mathtt{r}}} = \omega. \tag{4}$$

Thus by substituting these relationships in Lemma 3.1, we get

$$\mathrm{Coeff}\left(p(x)^{\frac{n\mathtt{l}}{\mathtt{r}}}, x^{n\mathtt{l}\omega}\right) = \frac{2p(x_\omega)^{\frac{n\mathtt{l}}{\mathtt{r}}}}{(x_\omega)^{n\mathtt{l}\omega} \sqrt{2\pi \frac{n\mathtt{l}}{\mathtt{r}} b_p(x_\omega)}} (1 + o(1)). \tag{5}$$

We summarize our results thus far.

Lemma 3.2: [Ensemble Average of Weight Distribution] Consider the regular LDPC ensemble $\mathbb{G}(n, \mathtt{l}, \mathtt{r})$. Define $h(\omega) = -(\omega \ln(\omega) + (1-\omega)\ln(1-\omega))$, where $\ln(\omega)$ is the natural logarithm of ω. Then for $\omega \in (0,1)$ such that $\mathtt{l}n\omega \in 2\mathbb{N}$,

$$\mathbb{E}[N(G, n\omega)] = \frac{2\sqrt{\mathtt{r}} e^{nW_{\mathrm{com}}(\omega)}}{\sqrt{2\pi n b_p(x_\omega)}} (1 + o(1)),$$

where $W_{\mathrm{com}}(\omega) = \frac{\mathtt{l}}{\mathtt{r}} \ln(p(x_\omega)) - (\mathtt{l}-1)h(\omega) - \mathtt{l}\omega \ln(x_\omega)$ and x_ω is the unique positive solution of equation (4). If $n\mathtt{l}\omega$ is odd, then $\mathbb{E}[N(G, n\omega)] = 0$.

Proof. We note that $n\mathtt{l}\omega$ must be even, otherwise $\mathbb{E}[N(G, n\omega)] = 0$ as $\mathrm{Coeff}\left(p(x)^{\frac{\mathtt{l}n}{\mathtt{r}}}, x^{n\mathtt{l}\omega}\right) = 0$ in (2). When $n\mathtt{l}\omega$ is even, using Stirling's approximation we get:

$$\binom{n}{n\omega} = \frac{e^{nh(\omega)}}{\sqrt{2\pi n\omega(1-\omega)}} (1 + o(1)). \tag{6}$$

By substituting (5) and (6) in (2), we get the desired result. □

To compute the second moment, we note that $\mathbb{E}[N^2(G, n\omega)] = \mathbb{E}[\sum_{w,w'} I_{w,w'}(G, n\omega)]$, where w, w' are both words of length n and weight $n\omega$ and

$$I_{w,w'}(G, n\omega) = \begin{cases} 1, & \text{if } w, w' \text{ are codewords of } G, \\ 0, & \text{otherwise.} \end{cases}$$

By definition of the ensemble, the expectation $\mathbb{E}[I_{w,w'}(G, n\omega)]$ does not depend on the specific choice of the pair w, w' but only on the cardinality of the overlap between the support sets of w and w'. In particular we can fix w to be a codeword of weight $n\omega$ with support set $\mathcal{W} = \{1, 2, \cdots, n\omega\}$, so that

$$\mathbb{E}[N^2(G, n\omega)] = \binom{n}{n\omega} \sum_{w'} \mathbb{E}[I_{w,w'}(G, n\omega)].$$

We can also fix w' for a given cardinality of overlap i with w to have support set $\mathcal{W}' = \{1, 2, \cdots, i, n\omega + 1, \cdots, 2n\omega - i\}$. Then,

$$\mathbb{E}[N^2(G, n\omega)] = \binom{n}{n\omega} \sum_{i=0}^{n\omega} \binom{n\omega}{i} \binom{n - n\omega}{n\omega - i} \mathbb{E}[I_{w,w'}(G, n\omega)].$$

The binomials inside the summation correspond to the number of words having cardinality of overlap with w equals to i. To calculate $\mathbb{E}[I_{w,w'}]$, we note that there are 3 different types of edges taking value 1. These types are: edges connected to $\mathcal{W}\cap\mathcal{W}'$, edges connected to $\mathcal{W}\backslash(\mathcal{W}\cap\mathcal{W}')$ and finally, edges connected to $\mathcal{W}'\backslash(\mathcal{W}\cap\mathcal{W}')$. A placement of edges is *valid* if each check node is connected to an even number of edges from $\mathcal{W}$ as well as from $\mathcal{W}'$, i.e., if the number of edges from each of the 3 different classes are *all* even or *all* odd. A moment's thought shows that the generating function for the number of valid placement is given by $f(x_1,x_2,x_3)^{\frac{n\mathtt{l}}{\mathtt{r}}} = f(\underline{x})^{\frac{n\mathtt{l}}{\mathtt{r}}}$, where x_1 corresponds to the number of edges connected to $\mathcal{W}\backslash(\mathcal{W}\cap\mathcal{W}')$, x_2 corresponds to the number of edges connected to $\mathcal{W}\cap\mathcal{W}'$ and x_3 corresponds to the number of edges connected to $\mathcal{W}'\backslash(\mathcal{W}\cap\mathcal{W}')$, and where $f(\underline{x})$ is the summation of the terms in the expansion of $(1+x_1+x_2+x_3)^{\mathtt{r}}$ which have powers of x_1,x_2 and x_3 either all even or all odd. Explicitly,

$$\begin{aligned} f(\underline{x}) &= \frac{1}{4}((1+x_1+x_2+x_3)^{\mathtt{r}}+(1+x_1-x_2-x_3)^{\mathtt{r}}) \\ &\quad +\frac{1}{4}((1-x_1+x_2-x_3)^{\mathtt{r}}+(1-x_1-x_2+x_3)^{\mathtt{r}}). \quad (7)\end{aligned}$$

Since there are $\mathtt{l}(n\omega-i)$ edges connected to $\mathcal{W}\backslash(\mathcal{W}\cap\mathcal{W}')$, $\mathtt{l}i$ edges connected to $\mathcal{W}\cap\mathcal{W}'$ and $\mathtt{l}(n\omega-i)$ edges connected to $\mathcal{W}'\backslash(\mathcal{W}\cap\mathcal{W}')$, we have

$$\begin{aligned}\mathbb{E}[I_{w,w'}(G,n\omega)] &= \mathrm{Coeff}\left(f(\underline{x})^{\frac{n\mathtt{l}}{\mathtt{r}}},x_1^{\mathtt{l}(n\omega-i)}x_2^{\mathtt{l}i}x_3^{\mathtt{l}(n\omega-i)}\right) \\ &\quad \frac{1}{(n\mathtt{l})!}((\mathtt{l}(n\omega-i))!)^2(\mathtt{l}i)!(n\mathtt{l}-2n\mathtt{l}\omega+\mathtt{l}i)!\end{aligned}$$

As all the edges are labeled, the factor $(n\mathtt{l})!$ corresponds to the total number of graphs in the ensemble $\mathbb{G}(n,\mathtt{l},\mathtt{r})$. The term $(\mathtt{l}(n\omega-i))!^2$ corresponds to interchanging the positions of edges connected to $\mathcal{W}\backslash(\mathcal{W}\cap\mathcal{W}')$, as well as to $\mathcal{W}'\backslash(\mathcal{W}\cap\mathcal{W}')$, $(\mathtt{l}i)!$ corresponds to interchanging the positions of edges connected to $\mathcal{W}\cap\mathcal{W}'$, and $(\mathtt{l}(n-2n\omega+i))!$ corresponds to interchanging of the positions of edges taking value 0. Hence,

$$\mathbb{E}[N^2(G,n\omega)] = \sum_{i=0}^{n\omega}\underbrace{\mathrm{Coeff}\left(f(\underline{x})^{n\mathtt{l}/\mathtt{r}},x_1^{\mathtt{l}(n\omega-i)}x_2^{\mathtt{l}i}x_3^{\mathtt{l}(n\omega-i)}\right)}_{C_i}$$

$$\underbrace{\frac{\binom{n}{n\omega}}{(n\mathtt{l})!}\binom{n\omega}{i}\binom{n-n\omega}{n\omega-i}((\mathtt{l}(n\omega-i))!)^2(\mathtt{l}i)!(\mathtt{l}(n-2n\omega+i))!}_{F_i} \quad (8)$$

Let S_i be the i^{th} summation term in (8), so $S_i = F_iC_i$. Note that $S_i = 0$ for $i < (2n\omega-n)^+$ as there can not exist two words of length n and weight $n\omega$ such that the cardinality of their overlap is less than $(2n\omega-n)^+$. To get a closed form expression for $\mathbb{E}[N^2(G,n\omega)]$, we use Stirling's formula to approximate the factorial terms and to approximate the Coeff function we use the following multidimensional extension of Lemma 3.1 as given in Theorem 2 of [1].

Lemma 3.3: [Multidimensional Saddle Point Method] Let $\underline{i} := (\mathtt{l}(n\omega-i),\mathtt{l}i,\mathtt{l}(n\omega-i))$, $\underline{j} := (\mathtt{l}(n\omega-j),\mathtt{l}j,\mathtt{l}(n\omega-j))$ and $0 < \lim_{n\to\infty} i/n < \omega$, $f(\underline{x})$ be as defined in (7) and $\underline{t} = (t_1,t_2,t_3)$ be a positive solution of $a(\underline{x}) = \frac{\mathtt{r}\underline{i}}{n\mathtt{l}}$, where $a(\underline{x}) = (\frac{x_i\partial f}{f\partial x_i})_{i=1}^3$. Then $\mathrm{Coeff}\left(f(\underline{x})^{\frac{n\mathtt{l}}{\mathtt{r}}},\underline{x}^{\underline{i}}\right)$ can be approximated using the saddle point method for multivariate polynomials,

$$\mathrm{Coeff}\left(f(\underline{x})^{\frac{n\mathtt{l}}{\mathtt{r}}},\underline{x}^{\underline{i}}\right) = \frac{4f(\underline{t})^{\frac{n\mathtt{l}}{\mathtt{r}}}}{(\underline{t})^{\underline{i}}\sqrt{(2\pi\frac{n\mathtt{l}}{\mathtt{r}})^3|B(\underline{t})|}}(1+o(1)),$$

where $B(\underline{x})$ is a 3×3 matrix whose elements are given by $B_{i,j} = x_j\frac{\partial a_i}{\partial x_j} = B_{j,i}$. Also, $\mathrm{Coeff}\left(f(\underline{x})^{\frac{n\mathtt{l}}{\mathtt{r}}},\underline{x}^{\underline{j}}\right)$ can be approximated in terms of $\mathrm{Coeff}\left(f(\underline{x})^{\frac{n\mathtt{l}}{\mathtt{r}}},\underline{x}^{\underline{i}}\right)$. This approximation is called the *local limit theorem* of $\underline{j}$ around $\underline{i}$. Explicitly, if $\underline{u} := \sqrt{\frac{\mathtt{r}}{n\mathtt{l}}}(\underline{j}-\underline{i})$ and $\|\underline{u}\| = O((\ln n)^{\frac{1}{3}})$, then

$$\begin{aligned}\mathrm{Coeff}\left(f(\underline{x})^{\frac{n\mathtt{l}}{\mathtt{r}}},\underline{x}^{\underline{j}}\right) &= \underline{t}^{\underline{i}-\underline{j}}\exp\left(-\frac{1}{2}\underline{u}.B(\underline{t})^{-1}.\underline{u}^T\right) \\ &\quad \mathrm{Coeff}\left(f(\underline{x})^{\frac{n\mathtt{l}}{\mathtt{r}}},\underline{x}^{\underline{i}}\right)(1+o(1)).\end{aligned}$$

Proof. We need to modify the proof of Theorem 2 of [1] to our case and is relegated to the appendix. □

The system of equations corresponding to $a(\underline{x}) = \frac{\mathtt{r}\underline{i}}{n\mathtt{l}}$ is symmetric in x_1 and x_3. Hence a positive solution $\underline{x}$ of this system of equations satisfies $x_1 = x_3$ and the system reduces to the following equations,

$$x_1\frac{(1+2x_1+x_2)^{\mathtt{r}-1}-(1-2x_1+x_2)^{\mathtt{r}-1}}{(1+2x_1+x_2)^{\mathtt{r}}+2(1-x_2)^{\mathtt{r}}+(1-2x_1+x_2)^{\mathtt{r}}} = \omega-\alpha, \quad (9)$$

$$x_2\frac{(1+2x_1+x_2)^{\mathtt{r}-1}-2(1-x_2)^{\mathtt{r}-1}+(1-2x_1+x_2)^{\mathtt{r}-1}}{(1+2x_1+x_2)^{\mathtt{r}}+2(1-x_2)^{\mathtt{r}}+(1-2x_1+x_2)^{\mathtt{r}}} = \alpha, \quad (10)$$

where $\alpha = \frac{i}{n}$.

In order to evaluate the second moment, we need to find the dominant terms of the summation in (8). To find all the dominant terms, let the term corresponding to $i = i_m$ i.e. $S_{i_m} = F_{i_m}C_{i_m}$ be a local maximum of $\{S_i\}_{i=0}^{n\omega}$. We assume that $0 < \lim_{n\to\infty} i_m/n < \omega$. We analyze the terms $S_{(2n\omega-n)^+}$ and $S_{n\omega}$ separately. Let $\Delta = i-i_m$ and $\alpha_m = i_m/n$. We expand F_i and C_i for $\Delta\in(-\sqrt{n}(\ln n)^{\frac{1}{3}},\sqrt{n}(\ln n)^{\frac{1}{3}})$ in terms of F_{i_m} and C_{i_m} using Stirling's approximation and the local limit theorem of Lemma 3.3 respectively. Then,

$$\begin{aligned}F_i &= F_{i_m}\exp\left(\Delta(\mathtt{l}-1)\ln\left(\frac{i_m(n-2n\omega+i_m)}{(n\omega-i_m)^2}\right)\right) \\ &\quad \exp\left(\frac{\Delta^2}{2n\sigma_F^2(\alpha_m)}\right)(1+O(\Delta^3/n^2)), \\ C_i &= C_{i_m}\exp\left(\Delta\mathtt{l}\ln\left(\frac{t_1^2}{t_2}\right)-\frac{\Delta^2}{2n\sigma_c^2(\alpha_m)}\right)(1+o(1)),\end{aligned}$$

where

$$\begin{aligned}F_{i_m} &= \left(\frac{(n\omega-i_m)^{2(n\omega-i_m)}i_m^{i_m}(n-2n\omega+i_m)^{n-2n\omega+i_m}}{n^n}\right)^{\mathtt{l}-1} \\ &\quad \mathtt{l}\sqrt{\mathtt{l}}(1+o(1)), \\ \frac{1}{\sigma_F^2(\alpha_m)} &= \left(\frac{2(\mathtt{l}-1)}{\omega-\alpha_m}+\frac{\mathtt{l}-1}{\alpha_m}+\frac{\mathtt{l}-1}{(1-2\omega+\alpha_m)}\right), \\ \sigma_c^2(\alpha_m) &= \frac{1}{\mathtt{l}\mathtt{r}((-1,1,-1).B(\underline{t})^{-1}.(-1,1,-1)^T)}. \quad (11)\end{aligned}$$

Hence,

$$S_i = \mathrm{S}_{i_m} \exp\left(\Delta\left((\mathtt{l}-1)\ln\left(\frac{i_m(n-2n\omega+i_m)}{(n\omega-i_m)^2}\right)+\mathtt{l}\ln\left(\frac{t_1^2}{t_2}\right)\right)\right)$$

$$\exp\left(\Delta^2\left(\frac{1}{2n\sigma_F^2(\alpha_m)}-\frac{1}{2n\sigma_c^2(\alpha_m)}\right)\right)(1+o(1)). \qquad (12)$$

We know that there is a local maximum at $\Delta = 0$, hence the coefficient of Δ in (12) will vanish. This gives an additional equation governing α_m:

$$\left(\frac{\alpha_m(1-2\omega+\alpha_m)}{(\omega-\alpha_m)^2}\right)^{\mathtt{l}-1} = \left(\frac{t_2}{t_1^2}\right)^{\mathtt{l}}. \qquad (13)$$

We solve (9), (10) and (13) and find all the solutions such that $0<\alpha_m<\omega$, $t_1>0$, $t_2>0$ and the coefficient of Δ^2 in (12) is negative (this ensures that S_{i_m} is a local maximum). One of the possible solution to this system of polynomial equations is $\alpha_m = \omega^2$. This is because $\{C_i\}_{i=0}^{n\omega}$ and $\{F_i\}_{i=0}^{n\omega}$ are concave and convex sequences respectively, both achieving their extreme values at $i = n\omega^2$. Hence $\{S_i\}_{i=0}^{n\omega}$ also achieves an extreme value at $i = n\omega^2$. If $\alpha_m = \omega^2$ is a unique global maximum in the solution set of (9), (10) and (13), then we can get a closed form expression for second moment. We summarize this in the following lemma.

Lemma 3.4: [Second Moment Method] Consider the regular LDPC ensemble $\mathbb{G}(n,\mathtt{l},\mathtt{r})$. Then for $\omega\in(0,1)$, if $W_{\mathrm{com}}(\omega)>0$ and if the following conditions are satisfied,

1) $\alpha_m = \omega^2$ is the only solution of (9), (10) and (13) for which coefficient of Δ^2 in (12) is negative,
2) $\lim_{n\to\infty}\ln(S_{n\omega^2})/n > \lim_{n\to\infty}\ln(S_{(2n\omega-n)^+})/n$,

then by the second moment method we have,

$$\lim_{n\to\infty}\mathrm{P}\left(1-\varepsilon\le\frac{N(G,n\omega)}{\mathbb{E}[N(G,n\omega)]}\le 1+\varepsilon\right)\ge 1-\frac{\delta(\omega,\mathtt{l},\mathtt{r})}{\varepsilon^2},$$

where

$$\delta(\omega,\mathtt{l},\mathtt{r}) = \frac{b_p(x_\omega)\sqrt{r}\sigma_F(\omega^2)\sigma_c(\omega^2)}{\sqrt{|B(x_\omega,x_\omega^2,x_\omega)|\,(\sigma_F^2(\omega^2)-\sigma_c^2(\omega^2))}}-1,$$

and x_ω is the only positive solution of (4).

Remark: Note that the conditions of Lemma 3.4 are hard to verify in general but they are typically easy to verify for any given regular LDPC ensemble.

Proof. We observe that the solution $\underline{t}$ of (9), (10) for $\alpha = \omega^2$ satisfies $t_2 = t_1^2$ and this system of equations reduces to a single equation which is identical to (4), the equation we need to solve to find $\mathbb{E}[N(G,n\omega)]$. Thus $t_1 = x_\omega$. By (12) and noting that the terms $S_{n\omega^2+\Delta}$ for $\Delta\notin(-\sqrt{n}(\ln n)^{\frac{1}{3}},\sqrt{n}(\ln n)^{\frac{1}{3}})$ are much smaller than $S_{n\omega^2}$, we get

$$\begin{aligned}\mathbb{E}[N^2(G,n\omega)] &= S_{n\omega^2}\sum_{\Delta=-\sqrt{n}(\ln n)^{\frac{1}{3}}}^{\sqrt{n}(\ln n)^{\frac{1}{3}}}\exp\left(\frac{-\Delta^2}{2\sigma_s^2}\right)(1+o(1)),\\ &= S_{n\omega^2}\int_{-\infty}^{\infty}\exp\left(\frac{-x^2}{2\sigma_s^2}\right)dx(1+o(1)),\\ &= S_{n\omega^2}\sqrt{2\pi\sigma_s^2}(1+o(1)),\\ \text{where}\quad \frac{1}{\sigma_s^2} &= \frac{1}{n\sigma_c^2(\omega^2)}-\frac{1}{n\sigma_F^2(\omega^2)}.\end{aligned}$$

To evaluate $S_{n\omega^2}$, we use Lemma 3.3, Stirling's approximation for factorial terms and observe that $f(x_\omega,x_\omega^2,x_\omega) = p(x_\omega)^2$. This gives,

$$\mathbb{E}[N^2(G,n\omega)] = \frac{4\sigma_c(\omega^2)\sigma_F(\omega^2)\mathtt{r}\sqrt{\mathtt{r}}e^{2nW_{\mathrm{com}}(\omega)}(1+o(1))}{2\pi n\sqrt{(\sigma_F^2(\omega^2)-\sigma_c^2(\omega^2))\,|B(x_\omega,x_\omega^2,x_\omega)|}}.$$

We need the condition $W_{\mathrm{com}}(\omega)>0$, as $\lim_{n\to\infty}\frac{\ln(S_{n\omega^2})}{n} = 2W_{\mathrm{com}}(\omega)$ and $\lim_{n\to\infty}\frac{\ln(S_{n\omega})}{n} = W_{\mathrm{com}}(\omega)$. Clearly when $W_{\mathrm{com}}(\omega)$ is negative, $S_{n\omega^2}$ can not be a global maximum. Now using Lemma 3.2 the second moment method gives us:

$$\lim_{n\to\infty}\mathrm{P}\left(1-\varepsilon\le\frac{N(G,n\omega)}{\mathbb{E}[N(G,n\omega)]}\le 1+\varepsilon\right) \ge 1-\frac{\delta(\omega,\mathtt{l},\mathtt{r})}{\varepsilon^2}.$$

This proves the lemma. □

The bound obtained in Lemma 3.4 can in general only be evaluated numerically except for the cases when (4) can be solved analytically, e.g., for the $(3,4)$-regular code.

IV. Discussion

Fix the relative weight ω. If $\varepsilon\in(0,1)$ then we conclude that asymptotically for at least a fraction $1-\frac{\delta(\omega,\mathtt{l},\mathtt{r})}{\varepsilon^2}$ of codes, the number of codewords $N(G,n\omega)$ (for a fixed ω) is at most a constant factor away from the ensemble average. Also from

$(\mathtt{l},\mathtt{r})$-code	ω_{min}	$1-\frac{\delta(\omega_{min},\mathtt{l},\mathtt{r})}{0.95^2}$
(3,6)	0.0227334	0.740611
(6,12)	0.0956337	0.963306
(12,24)	0.109404	0.999617
(24,48)	0.110026	$\sim$1.0

TABLE I: $\lim_{\omega\to\omega_{min}+}1-\frac{\delta(\omega,\mathtt{l},\mathtt{r})}{\varepsilon^2}$ for rate $=\frac{1}{2}$ and $\varepsilon=0.95$

Fig. 1 we see that $1-\frac{\delta(\omega,\mathtt{l},\mathtt{r})}{\varepsilon^2}$ is an increasing function of ω for $\omega\in(\omega_{min},1/2)$ and is a decreasing function for $\omega>1/2$. It is equal to 1 for $\omega=1/2$. This implies that asymptotically in almost all the codes there are $\mathbb{E}[N(G,n/2)](1\pm\varepsilon)$ codewords of weight $n/2$. For ω close to the typical minimum distance ω_{min}, the bound stays nontrivial. In Table 1, $\lim_{\omega\to\omega_{min}+}1-\frac{\delta(\omega_{min},\mathtt{l},\mathtt{r})}{\varepsilon^2}$ is given for regular codes of rate=$\frac{1}{2}$ and $\varepsilon=0.95$. We observe that if we fix the rate and let $\mathtt{l}$ and $\mathtt{r}$ increase then the bound approaches 1 for all ω for which $W_{\mathrm{com}}(\omega)$ is positive. This implies that for regular ensembles with large left and right degree almost all the codes have a weight distribution which is very close to the ensemble average. We see that the second

moment method can capture the concentration property of the weight distribution for regular ensembles with large left and right degrees. However for the regular ensembles in general it fails to do so.

Acknowledgment: The author wishes to thank Rüdiger Urbanke for many helpful discussions and suggestions on the preparation of the paper.

REFERENCES

[1] E. A. Bender and L. B. Richmond, *Central and local limit theorems applied to asymptotic enumeration II: multivariate generating functions*, J. Combin. Theory Ser. A 34 (1983), pp. 255-265.

[2] S. Condamin, *Study of the weight enumerator function for a Gallager code*, project report, Cavendish Laboratory, University of Cambridge, July 2002.

[3] D. Burshtein and G. Miller, *Asymptotic enumeration methods for analyzing LDPC codes*, IEEE Transactions on Information Theory, Volume: 50, Issue: 6, June 2004.

[4] C. Di, A. Montanari, R. Urbanke, *Weight distribution of LPDC code ensemble: combinatorics meets statistical physics*,in International Symposium on Information Theory Proceedings, 27 June-2 July 2004, Pages:102.

[5] C. Di, T. Richardson, R. Urbanke, *Weight distribution of iterative coding systems: How deviant can you be?*, in International Symposium on Information Theory, Washington, D.C., June 2001, IEEE, p. 50.

[6] P. Flajolet, R. Sedgewick, *Analytic Combinatorics* preprint.

[7] R. G. Gallager, *Low-Density Parity-Check Codes*, M. I. T. Press, Cambridge, Massachusetts, 1963.

[8] S. Litsyn and V. Shevelev, *On Ensembles of Low-Density Parity-Check Codes: Asymptotic Distance Distributions*, IEEE Transactions on Information Theory, Vol. 48, No. 4, April 2002.

[9] A. Montanari, *The Glassy Phase of Gallager Codes*, European Physics Journal, 23 (2001).

[10] S. Van Mourik, D. Saad, Y. Kabashima, *Critical noise levels for LDPC decoding*, Physical Review E, 66 (2002).

[11] N. Sourlas, *Spin-glass models as error-correcting codes*, Nature, 339 (1989), pp. 693-695.

[12] N. Sourlas, *Spin glasses, error-correcting codes and finite-temperature decoding*, Europhysics Letters, 25 (1994), pp. 159-164.

[13] A. Vardy, *The intractability of computing the minimum distance of code*, IEEE Transaction on Information Theory, 43 (1997), pp. 1757-1766.

V. APPENDIX

We modify the proof of Theorem 2 of [1] to prove Lemma 3.3. Let $\varphi_n(\underline{z}) = f(\underline{z})^{\frac{n\mathtt{l}}{\mathtt{r}}}$, $I = \sqrt{-1}$ and we denote an interval of the form $[-a,a]^3$ by $R(a)$. We also expand $\varphi_n(\underline{z})$ as $\varphi_n(\underline{z}) = \sum_{\underline{k}} a_n(\underline{k}) z^{\underline{k}}$. Let $\underline{t}$ be the positive solution of $a(\underline{x}) = \frac{\mathtt{r}\underline{j}}{n\mathtt{l}}$. From the inverse Fourier transform, we get

$$\frac{1}{(2\pi)^3}\int_{R(\pi)} \frac{\varphi_n(\underline{t}e^{I\underline{v}})}{\varphi_n(\underline{t})} e^{-I\underline{j}.\underline{v}^T} d\underline{v} = \frac{a_n(\underline{j})\underline{t}^{\underline{j}}}{\varphi_n(\underline{t})}. \tag{14}$$

We recall that the Fourier transform of a Gaussian is Gaussian,

$$\int_{R(\infty)} e^{-I\underline{u}.\underline{s}^T - \frac{\underline{s}.B(t).\underline{s}^T}{2}} d\underline{s} = \sqrt{\frac{(2\pi)^3}{|B(\underline{t})|}} e^{-\frac{1}{2}\underline{u}.B(\underline{t})^{-1}.\underline{u}^T}. \tag{15}$$

Also for any function $K(n)$ growing with n,

$$\left| \int_{R(K(n))} e^{-I\underline{u}.\underline{s}^T - \frac{\underline{s}.B(t).\underline{s}^T}{2}} d\underline{s} - \int_{R(\infty)} e^{-I\underline{u}.\underline{s}^T - \frac{\underline{s}.B(t).\underline{s}^T}{2}} d\underline{s} \right| = O\left(\frac{1}{K(n)}\right). \tag{16}$$

We would like to show that for $n \to \infty$

$$\left| \left(\frac{n\mathtt{l}}{\mathtt{r}}\right)^{\frac{3}{2}} \int_{R(\pi)} \frac{\varphi_n(\underline{t}e^{I\underline{v}})}{\varphi_n(\underline{t})} e^{-I\underline{j}.\underline{v}^T} d\underline{v} - 4\sqrt{\frac{(2\pi)^3}{|B(\underline{t})|}} e^{-\frac{1}{2}\underline{u}.B(\underline{t})^{-1}.\underline{u}^T} \right| = o(1). \tag{17}$$

To prove this, we write $\varphi_n(\underline{t}e^{I\underline{v}})$ in exponential-log form and take the Taylor series expansion of the exponent around $\underline{v} = 0$,

$$\varphi_n(\underline{t}e^{I\underline{v}}) = e^{\left(\frac{n\mathtt{l}}{\mathtt{r}}\left(\ln(f(\underline{t}))+Ia(\underline{t}).\underline{v}^T - \frac{\underline{v}.B(\underline{t}).\underline{v}^T}{2} + O(\|\underline{v}\|^3)\right)\right)}. \tag{18}$$

Note that as $\ln(\varphi_n(\underline{z}))$ is analytic, so all the third order partial derivative of $\varphi_n(\underline{t}e^{I\underline{v}})$ are bounded. We partition the interval $R(\pi)$ into $R(\delta), R_1 = [-\delta,\delta]\times[\pi-\delta,\pi+\delta]^2, R_2 = [\pi-\delta,\pi+\delta]\times[-\delta,\delta]\times[\pi-\delta,\pi+\delta], R_3 = [\pi-\delta,\pi+\delta]^2\times[-\delta,\delta], R_4 = R(\pi)/(R(\delta)\cup R_1\cup R_2\cup R_3)$. Here δ can be any decaying function of n which satisfies that as $n\to\infty$ then $n\delta^2\to\infty$ and $n\delta^3\to 0$. We choose $\delta = n^{-\frac{2}{5}}$. By the symmetry of $f(\underline{x})$, $\varphi_n(x_1,x_2,x_3) = \varphi_n(x_1,-x_2,-x_3) = \varphi_n(-x_1,x_2,-x_3) = \varphi_n(-x_1,-x_2,x_3)$.

$$\int_{R(\delta)} \frac{\varphi_n(\underline{t}e^{I\underline{v}})}{\varphi_n(\underline{t})} e^{-I\underline{j}.\underline{v}^T} d\underline{v} = \int_{R_k} \frac{\varphi_n(\underline{t}e^{I\underline{v}})}{\varphi_n(\underline{t})} e^{-I\underline{j}.\underline{v}^T} d\underline{v},\ k\in\{1,2,3\},$$
$$\overset{\substack{a(\underline{t})=\frac{\mathtt{r}\underline{i}}{n\mathtt{l}}\\ (18)}}{=} \int_{R(\delta)} e^{I(\underline{i}-\underline{j}).v^T - \frac{\underline{l}n}{2\mathtt{r}}\underline{v}.B(\underline{t}).\underline{v}^T + O(n\delta^3)} d\underline{v}. \tag{19}$$

By the change of variable $\underline{y} := \sqrt{\frac{n\mathtt{l}}{\mathtt{r}}}$ in (19) and using (15,16), we get

$$\int_{R(\delta)} \frac{\varphi_n(\underline{t}e^{I\underline{v}})}{\varphi_n(\underline{t})} e^{-I\underline{j}.\underline{v}^T} d\underline{v} =$$
$$\left(\frac{\mathtt{r}}{n\mathtt{l}}\right)^{\frac{3}{2}} \sqrt{\frac{(2\pi)^3}{|B(\underline{t})|}} e^{-\frac{\underline{u}.B(\underline{t})^{-1}.\underline{u}^T}{2}} (1+O(n^{-\frac{1}{5}})) + \left(\frac{\mathtt{r}}{n\mathtt{l}}\right)^{\frac{3}{2}} O(n^{-\frac{1}{10}}).$$

Now to evaluate the integral over R_4, let $f(\underline{t}) = \sum_{\underline{k}} b(\underline{k})\underline{t}^{\underline{k}}$ and recall that $f(\underline{t})$ is a 3-variable polynomial of finite degree. Then by some algebraic manipulation we get,

$$\left|\frac{f(\underline{t}e^{I\underline{v}})}{f(\underline{t})}\right|^2 = 1 - \frac{\sum_{\underline{k}\neq\underline{l}} b(\underline{k})b(\underline{l})\underline{t}^{\underline{k}+\underline{l}}(1-\cos\left((\underline{k}-\underline{l}).v^T\right)}{f(\underline{t})^2}$$

Also $f(\underline{t})$ has $1, t_1^2, t_2^2, t_3^2$ as its summation terms and in R_4 at least one of the variable v_k satisfies $v_k \notin [-\delta,\delta]$ where $k\in\{1,2,3\}$. This implies that for some positive constants c, c_1,

$$\int_{R_4} \left|\frac{f(\underline{t}e^{I\underline{v}})}{f(\underline{t})}\right|^{\frac{n\mathtt{l}}{\mathtt{r}}} d\underline{v} \le \pi^3(1-c_1\delta^2)^{\frac{n\mathtt{l}}{2\mathtt{r}}} = \pi^3(1-c_1 n^{-\frac{4}{5}})^{\frac{n\mathtt{l}}{2\mathtt{r}}}$$
$$= O(e^{-cn^{\frac{1}{5}}}).$$

By combining the above steps we get,

$$\left| \left(\frac{n\mathtt{l}}{\mathtt{r}}\right)^{\frac{3}{2}} \int_{R(\pi)} \frac{\varphi_n(\underline{t}e^{I\underline{v}})}{\varphi_n(\underline{t})} e^{-I\underline{j}.\underline{v}^T} d\underline{v} - 4\sqrt{\frac{(2\pi)^3}{|B(\underline{t})|}} e^{-\frac{1}{2}\underline{u}.B(\underline{t})^{-1}.\underline{u}^T} \right| = O(n^{-\frac{1}{10}}),$$

$$\left| \left(\frac{n\mathtt{l}}{\mathtt{r}}\right)^{\frac{3}{2}} \frac{(2\pi)^3 a_n(\underline{j})\underline{t}^{\underline{j}}}{\varphi_n(\underline{t})} - 4\sqrt{\frac{(2\pi)^3}{|B(\underline{t})|}} e^{-\frac{1}{2}\underline{u}.B(\underline{t})^{-1}.\underline{u}^T} \right| \overset{(14)}{=} O(n^{-\frac{1}{10}}) \tag{20}$$

The approximation of $\mathrm{Coeff}(f(\underline{x})^{\frac{n\mathtt{l}}{\mathtt{r}}}, \underline{x}^{\underline{i}})$ is obtained by substituting $\underline{j} = \underline{i}$ (which implies $\underline{u} = (0,0,0)$) in (20). Also for the local limit theorem to hold we need in (20) that $e^{\frac{1}{2}\underline{u}.B_f(\underline{t})^{-1}.\underline{u}^T} n^{-\frac{1}{10}} = o(1)$. For our application choosing $\|\underline{u}\| = O((\ln n)^{\frac{1}{3}})$ suffices.